Sensitive Metadata Analytic Collaboration (SMAC)
Concept of Operations
October 2006

Background
In June 2004 via the Alice Springs Resolution (ASR), the SIGINT Agency Heads agreed to the development of a system to provide a single query access to all metadata repositories across the Australian, Canadian, New Zealand, United Kingdom and United States Signals Intelligence community. The concept was reiterated in 2005 June in the Cheltenham Resolution and a solid commitment to action was undertaken by NSA and GCHQ after the London bombings in July 2005 (when unprecedented sensitive metadata sharing occurred). That "system" was substantiated in the Sensitive Metadata Analytic Collaboration (SMAC), a collaborative 5-Eyes team furthering the SIGINT mission by performing analysis and enabling optimal use of sensitive metadata. This Concept of Operations will define the purpose, organizational structure, scope and procedures of SMAC. It will also project to a possible future state.

Purpose
The practical implementation of the vision stated in the ASR requires policy, legal and technical coordination between the partners. Furthermore, it requires cultural change. SMAC will work with related delivery mechanisms to jointly address these coordination and cultural issues to achieve the sharing goal.

Vision
In collaboration with our foreign partners, further the SIGINT mission by performing analysis and enabling optimal use of sensitive metadata.

Organizational Structure
When an employee is selected to participate in SMAC, they are indoctrinated into SMAC by the SMAC Lead and their National Steering Committee member. Only those members who have been briefed to the SMAC process can participate in SMAC activities. This is required to educate the participant in the sensitivities involved in the SMAC process to assure all equities are protected.

Steering Committee
Membership: One senior-level person from each of the 5-Eyes Agencies.
Role: Ensure effective and authorized operation of the SMAC analytic team on behalf of the 5-Eyes community.
Responsibilities:

- authorizing SMAC business lines
- ensuring national authorization for release of SMAC products into the Intelligence Community (IC)
- advocating SMAC within National Agency and ensuring stakeholder buy-in

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 22012031

- providing prioritization guidelines
- providing strategic guidance on the issues affecting national contribution to the SMAC analytic team
- tasking National Agency to ensure effective resolution of any issues identified by SMAC analytic team; tracking those actions
- reporting on SMAC analytic team progress (including metrics) to respective seniors
- resourcing the SMAC analytic team
- meet quarterly

SMAC Analytic Team

Membership: At least one representative from each of the 5-Eyes Agencies, fully cleared to access all metadata from National holdings and knowledgeable about national sensitive collection.

Role: Ensure effective and appropriate handling of and response to SMAC tasking, on behalf of the 5-Eyes community.

Responsibilities:

- Respond to tasking by ensuring: complete and timely results, within the timescales requested; timely dissemination of SMAC products to all interested parties; protection of National sensitivities in communication of SMAC work; unresolved issues around 5-Eyes sharing are known to the Steering Committee.
- Act as a conduit for National Agency tasking by: effectively communicating the task, its priority, and any sensitivities to ensure other partners can respond; contribute to agreement on approved dissemination of the results with the requesting Agency/community; tracking timeliness of the response; obtain and collate feedback for the contributing Agencies to derive value-added statistics; track and document tasking and results; educate analysts within National Agency on SMAC and its contribution to the SIGINT mission.
- Develop expertise on metadata resources by: developing an understanding of National metadata resources and the associated legal, policy and technical restrictions on sharing; negotiating the approved dissemination of this information in response to mission needs.
- Identify barriers to sharing and business process improvement by: highlighting issues restricting sharing of operationally relevant metadata, with recommendations for improvement; ensuring that SMAC processes do not become a cottage industry through migration of successful business processes into main business lines.
- Appropriately handle sensitive communications involved in SMAC daily operations to maintain the trust required for sharing sensitive information between the partners. This has been referred to as “SMAC Channels Only”.

Intelligence Community

SMAC was established by the SIGINT Directors to improve sharing of sensitive metadata among the 5-Eyes SIGINT Community. Since this is an agreement amongst the SIGINT Directors, the formal agreement does not extend to other members of the

Intelligence Community (IC). It is recognized that SIGINT does not work in a vacuum and that there is benefit to expanding the collaboration to include other members of the IC. Each Nation will manage this inclusion process with coordination and cooperation of all members of SMAC. The SIGINT partners are a model for collaboration at a level of trust that is not enjoyed by other IC partners. SMAC can be used as an avenue to demonstrate the power of collaboration, but this path must be taken slowly with caution and respect for all involved. This is not to say that selectors from our other partners cannot be submitted to the SMAC RFI process at the discretion of the SMAC National representative. These "sensitive" selectors will be protected by SMAC according to the handling caveats mandated by the National representative.

Scope of Mission

SMAC has both tactical and strategic objectives which are both being aggressively pursued. The tactical objective is implemented predominately through the Request for Information (RFI) process which leads to systemic changes. The strategic objective is implemented through results from the investigative nature of the team. Strategic initiatives will sometimes be the result of the outcome of tactical actions and other times the result of highlighting barriers to sharing that have been identified.

Regardless of the nature of the action, tactical or strategic, the sensitivity of the information provided is dictated by the National representative and honored by the SMAC team. Selectors, results of queries against those selectors, operational information regarding the task, … each aspect is protected according to the instructions determined by the National representative. Adherence to this practice must be absolute.

<u>Tactical Procedures:</u>

SMAC has established an RFI process that is documented on the SMAC web page, accessible by all 5-Eyes partners. The process is initiated by the completion of a Request Form (Appendix A) by any analyst desiring the sensitive source metadata available. The NSA process after an RFI submission is documented in Appendix B. There is a slight variation of this process for the other SMAC members, but the concept of sensitive information being accepted into SMAC ("sensitive in") and the potential for sensitive information being provided back to the requestor ("sensitive out") is one which is adhered to by all SMAC participants. Information on the process is also available to analysts in the Frequently Asked Questions (FAQ) document on the web page (Appendix C). The National SMAC representative lists the RFI in a spreadsheet (Appendix D) and tracks the outcome and feedback. Feedback is requested for all SMAC RFIs using a SMAC feedback form (Appendix E).

Given that the current status of SMAC does not include physical representation of National representatives for all 5-Eyes having access to all sensitive metadata repositories at NSAW, procedures for handling SMAC requests include the transfer of information back to a SMAC point person back at their Agency. This point person handles the request and does not distribute the information further internally, and returns the results back to the SMAC National representative here at NSAW.

Since SMAC has taken on the responsibility for the 24 hour/ 7 days per week ability to respond to tactical operational requirements, previously owned by the now-defunct JINTAC, a procedure to execute this capability must be established and implemented.

SMAC Responsibilities in Threat-to-life Scenarios

(S//FVEY) In the effort to maximize the amount of metadata shared between the 5-EYES, SMAC developed an RFI process allowing analysts from any of the 5-EYES to request sanitized and/or minimized metadata on strong selectors from sources not automatically shared to support sensitive operations. Within this RFI process, information outlining analytic motivation behind the targeting and the timeliness is provided by the requestor to the SMAC national representative. This information is often shared without fear of further distribution amongst the trusted 5-EYES SMAC team and can contain analysis indicating threat-to-life. In most situations, this would mandate that each of the SMAC analysts take action to initiate their national process for notifying the appropriate people about the imminent threat but in this case, it is only the responsibility of the requester to make their superiors aware of the threat. Should SMAC take this action, it could potentially jeopardize ongoing operations; the SMAC analyst needs to be exempt from invoking the normal Threat-to-Life process defined by their SIGINT agency.

(S//FVEY) SMAC provides 5-EYES analysts with access to sensitive or routinely unshared target-related information held by second parties. It is ultimately the responsibility of the requesting agency to disseminate information via the appropriate channel/s from this or any subsequent further analysis that either suggests or indicates that there is an imminent or immediate threat to human/s life of a citizen/s of a second party Agency. SMAC bears no responsibility to disseminate information indicating a Threat-to-Life. The requesting agency analyst need refer to their respective Inter-Agency policy for guidance for Threat-to-Life reporting requirements.

Strategic Procedures:

Marketing SMAC

Marketing of the SMAC capability had been done in a variety of forums and this effort will continue for the duration of the SMAC mission.

Briefings

Briefings to management teams, at major annual conferences (A&P, SIGDEV, European SIGDEV, …) at educational seminars, and influential individuals are examples of attempts to educate the 5-Eyes community on SMAC.

Face-to-Face Communications

Visits to each of the 5-Eyes should be conducted to reinforce local communication about SMAC. Personal interaction at the office level for specific targets must be regularly undertaken.

Documentation

Quarterly reports will be written to document the status of SMAC activities. These reports are to be distributed to the Analytic Team and Steering Committee, and the Steering Committee may distribute in their National Agency as they deem appropriate. SMAC has a *web page* that is accessible by all members of the 5-Eyes. Information there includes the SMAC mission, points of contacts, forms to submit RFIs, FAQs, a single-

page *fact sheet*, and listing of relevant documents (strategies, legal and policy papers) on sharing metadata in the 5-Eyes community.
A *Business Plan* will be written to include an IT infrastructure outline and a budget for the near term and out years to maintain the SMAC capability.

Future of SMAC

Phase One

Phase one of the implementation of SMAC is dominated by the successful completion of a process to handle the tactical aspects of the mission need. The RFI process should be robust and fail-proof. Metrics used to measure the success of the RFI process include:

- Track the origin of the sensitive metadata (while protecting the source) so the value of the source can be measured;
- The source of the requestor by Agency and organization within the Agency;
- The number of times an Agency provided unique contributions;
- The number of DNR requests for which SMAC provided unique metadata;
- The number of DNI requests for which SMAC provided unique metadata;
- The number of overall RFIs submitted, differentiated by Agency;

This success will lead to the identification of barriers which need to be addressed to facilitate systemic change to enhance the mission. The completion of phase one will be judged by statistics generated by the SMAC Analytic Team and the continuation of support by the Steering Committee.

Phase Two

Phase two of the implementation of the SMAC concept will require an enhancement of the current effort and will focus more on the collaborative and investigative aspects of the uniqueness of the 5-Eyes team. SMAC, the method for sharing sensitive metadata, will be but one element of the new effort.
SMAC will undertake the 5-Eyes requirements identified by the SIGINT Directors as well as others. For instance, at the Pre-Chesapeake Meeting 2006, the following requirements could be absorbed into the SMAC mission:

- #8. (S//SI) Explore development of “ground rules” for secondary sharing (beyond SIGINT community) and dissemination of metadata to counter potentially revealing sources and methods.
- #9. (S//SI) Examine the policy and legal issues that prevent the sharing of metadata among the 5-Eyes partners. (SMAC already does this.)

Plan for SMAC Failure

Plans need to be in place to address the following potential SMAC “Failures”:

- Lack of participation by each of the 5-Eyes;
- Information that can and should be shared using the SMAC system which is not shared for one reason or another;
- Lack of trust between the 5-Eyes partners.

The current plan to address these types of failures is to use the Steering Committee to address the issues first and then, if not successful, raise the issue to their leadership at their National Agencies. The leaders of each of National Agencies would then provide suggestions for actions, which the Steering Committee and/or SMAC would undertake to resolve the issue.